

Vid frågor, kontakta: Daniel Hellström, Axalon Tech  
[daniel.hellstrom@axalon.se](mailto:daniel.hellstrom@axalon.se)  
+46 76-677 03 53

## Innehållsförteckning

|                              |   |
|------------------------------|---|
| Åtkomstmetod .....           | 2 |
| Skapa en Azure AD app .....  | 2 |
| Registrera appen .....       | 2 |
| Ladda upp certifikatet ..... | 4 |
| Tilldela behörigheter .....  | 5 |

## Åtkomstmetod

För att låta pluginet få åtkomst till SharePoint använder vi oss av en Azure AD app med ett certifikat. Behörigheten sätts sedan till de siter som pluginet ska kunna komma åt.

## Skapa en Azure AD app

Appen måste först registreras i erat Azure. Sedan måste behörigheter tilldelas och ett certifikat laddas upp.

Registrera appen

1. Logga in på <https://portal.azure.com> och gå till Azure AD.
2. Registrera en app.

The screenshot shows the Azure Active Directory portal interface. The header displays 'ollodev | Appregistreringar' and 'Azure Active Directory'. The left sidebar contains navigation options: 'Översikt', 'Komma igång', 'Förhandsversionshub', 'Diagnosticera och lösa problem', 'Hantera' (with sub-items: 'Användare', 'Grupper', 'External Identities', 'Roller och administratörer', 'Administrativa enheter', 'Företagsprogram', 'Enheter', 'Appregistreringar', 'Identitetsstyrning'). The 'Appregistreringar' item is highlighted with a red circle. The main content area shows a '+ Ny registrering' button, also highlighted with a red circle, and a search bar with the text 'Start typing a display name to filter these results'. There are also two informational messages in the main area.

3. Namnge appen och kryssa i att endast konton i eran organisation får åtkomst till appen.

Microsoft Azure

Start > ollodev >

## Registrera ett program

\* Namn

Det här programmets användarinriktade visningsnamn (du kan ändra det senare).

Kontotyper som stöds

Vem som kan använda det här programmet eller få åtkomst till det här API:et?

- Endast konton i den här organisationskatalogen (endast ollodev – enskild klientorganisation)
- Konton i valfri organisationskatalog (valfri Azure AD-katalog – flera klientorganisationer)
- Konton i valfri organisationskatalog (valfri Azure AD-katalog – flera klientorganisationer) och personliga Microsoft-konton (t.ex. Skype, Xbox)
- Endast personliga Microsoft-konton

[Hjälp mig att välja...](#)

Omdirigerings-URI (valfritt)

Vi returnerar autentiseringsvaret till den här URI:n efter att användaren har autentiserats. Att tillhandahålla det nu är valfritt och det kan ändras senare. Det krävs dock ett värde för de flesta autentiseringsscenarier.

Webben

4. Under appens översikt finns det ett Program-ID. Klipp ut det och maila den till Axalon.

**AxalonSPApp**

Sök (Ctrl+/) << Ta bort Slutpunkter Förhandsversionsfunktioner

- Översikt**
- Snabbstart
- Integrationsassistenten

Hantera

- Anpassning
- Autentisering
- Certifikat och hemligheter

**Information**

Visningsnamn : AxalonSPApp

**Program-ID (klient) : c93f8c9c-d09b-414d-80cd-9282de6b9263**

Katalog-ID (klientorganis... : 2f020602-934e-4d67-a10a-c8ca6c179e6d

Objekt-ID : c0181936-8746-4a48-a617-3c849200bf79

Från och med 30 juni 2020 lägger vi inte längre till några nya funktioner i ADAL uppdateras till MSAL (Microsoft Authentication Library) och Microsoft Graph.

Ladda upp certifikatet

1. Ni ska av Axalon ha fått certifikatet "SP2c8Plugin.cer", ladda upp det.

Start > Axalon | Appregistreringar > Axalon SP app

### Axalon SP app | Certifikat och hemligheter

Sök

Har du någon feedback?

Översikt

Snabbstart

Integrationsassistenten

Diagnostisera och lös problem

Hantera

- Anpassning och egenskaper
- Autentisering
- Certifikat och hemligheter**
- Tokenkonfiguration
- API-behörigheter
- Exponera ett API
- Approller
- Ägare

Autentiseringsuppgifter gör det möjligt för konfidentiell adresserbar webbplats (med ett HTTPS-schema). Om du klienthemlighet) som en autentiseringsuppgift.

Programregistreringscertifikat, hemligheter och feder

**Certifikat (0)** Klienthemligheter (0) Federera

Certifikat kan användas som hemligheter för att verifier nycklar.

Överför certifikat

| Tumavtryck   | Beskrivning |
|--|-------------|
| Inga certifikat har lagts till för det här programmet. |             |

### Överför certifikat

Överför ett certifikat (offentlig nyckel) med någon av följande filtyper: .cer, .pem, .crt \*

"SP2c8Plugin.cer"

Beskrivning

Ange en beskrivning för mallen

## Tilldela behörigheter

1. Gå till API-behörigheter

The screenshot shows the 'AxalonSPApp | API-behörigheter' management page. On the left is a navigation menu with 'API-behörigheter' selected and circled in red. The main content area features a search bar, a refresh button, and a notification: 'Administratören har beviljats med...'. Below this is the 'Konfigurerade behörigheter' section, which includes a '+ Lägg till en behörighet' button (circled in red), a table of permissions under 'Microsoft Graph (1)', and a 'User.Read' entry. At the bottom, there is a link to 'Testa Enterprise-program om du vill vis'.

Sök (Ctrl+/) << Uppdatera | Har du någor

Översikt  
Snabbstart  
Integrationsassistenten

Antera

Anpassning  
Autentisering  
Certifikat och hemligheter  
Tokenkonfiguration  
**API-behörigheter**  
Exponera ett API  
Approller | Förhandsversion  
Ägare

Administratören har beviljats med

Konfigurerade behörigheter

Program har behörighet att anropa API behörigheter ska innehålla alla behörig

+ Lägg till en behörighet ✓ Bev

Namn på API/behörigheter

Microsoft Graph (1)

User.Read


Testa Enterprise-program om du vill vis


- Lägg till Programbehörigheter mot SharePoint.

## Request API permissions ×

[← All APIs](#)

 **SharePoint**  
<https://microsoft.sharepoint-df.com/> [Docs](#) [↗](#)

 You and the users of your application may need a subscription for SharePoint. Users without a subscription may not be able to access all the features of this API. ×

 SharePoint APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead. ×

What type of permissions does your application require?

**Delegated permissions**  
 Your application needs to access the API as the signed-in user.

**Application permissions**  
 Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

| Permission  | Admin consent required                                 |
|---|--|
| <p>∨ <b>Sites (1)</b></p> <p><input type="checkbox"/> Sites.FullControl.All ⓘ<br/>Have full control of all site collections</p> <p><input type="checkbox"/> Sites.Manage.All ⓘ<br/>Read and write items and lists in all site collections</p> <p><input type="checkbox"/> Sites.Read.All ⓘ<br/>Read items in all site collections</p> <p><input type="checkbox"/> Sites.ReadWrite.All ⓘ<br/>Read and write items in all site collections</p> <p><input checked="" type="checkbox"/> Sites.Selected ⓘ<br/>Access selected site collections</p> | <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> |
| <p>∨ <b>TermStore (1)</b></p> <p><input type="checkbox"/> TermStore.Read.All ⓘ<br/>Read managed metadata</p> <p><input checked="" type="checkbox"/> TermStore.ReadWrite.All ⓘ<br/>Read and write managed metadata</p>   | <p>Yes</p> <p>Yes</p>                                  |
| <p>∨ <b>User (1)</b></p> <p><input checked="" type="checkbox"/> User.Read.All ⓘ<br/>Read user profiles</p> <p><input type="checkbox"/> User.ReadWrite.All ⓘ<br/>Read and write user profiles</p>  | <p>Yes</p> <p>Yes</p>                                  |

## 2. Nästa steg är att bevilja behörigheterna

### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission  Grant admin consent for Standardkatalog

| API / Permissions name  | Type        | Description                      | Admin consent requ... | Status                          |
|-------------------------|-------------|----------------------------------|-----------------------|---------------------------------|
| Microsoft Graph (1)     |             |                                  |                       | ...                             |
| User.Read               | Delegated   | Sign in and read user profile    | No                    | ...                             |
| SharePoint (3)          |             |                                  |                       | ...                             |
| Sites.Selected          | Application | Access selected site collections | Yes                   | ⚠ Not granted for Standar... ** |
| TermStore.ReadWrite.All | Application | Read and write managed metadata  | Yes                   | ⚠ Not granted for Standar... ** |
| User.Read.All           | Application | Read user profiles               | Yes                   | ⚠ Not granted for Standar... ** |

## 3. Sista steget är att ge appen rättigheter att läsa med nedanstående powershell script. Ändra variablerna till era egna.

Kontrollera att kontot som kör scriptet är site-admin över siten. Scriptet kräver även Powershell 7.2 och modulen PnP.PowerShell. Om du behöver installera modulen så görs det med kommandot `Install-Module PnP.PowerShell`.

Från och med 9 september 2024 är det inte längre möjligt att köra kommandot Connect-PnPOnline med parametern -Interactive utan att registrera en app i Microsoft Entra.

Du kan göra det med följande Powershell-kommando

```
Register-PnPEntraIDAppForInteractiveLogin -ApplicationName "PnP PowerShell" -SharePointDelegatePermissions "AllSites.FullControl" -Tenant axalon.onmicrosoft.com -Interactive
```

Använd AzureAppId i variabeln \$PnPEntraAppId nedan.

Här kommer en länk till en artikel som beskriver det mer i detalj

[PnP PowerShell - AADSTS700016: Application with identifier '31359c7f-bd7e-475c-86db-fdb8c937548e' was not found in the directory - SharePoint Diary](#)

```
$appId = "c1445902-6d66-46e2-a33f-d767f7f1afdb"
$siteCollUrl =
$appDisplayName = "Axalon SP app"
$PnPEntraAppId =

write-host "Connecting to your site."
Connect-PnPOnline -Url $siteCollUrl -Interactive -ClientId $PnPEntraAppId

write-host "Granting app $appDisplayName access"
#Granting app Read permission to the site collection.
Grant-PnPazureADAppSitePermission -Permissions "Read" -Site $siteCollUrl -AppId $appId -DisplayName $appDisplayName
```